



[Subscribe](#) (Full Service) [Register](#) (Limited Service, Free) [Login](#)

Search: ☒ The ACM Digital Library ☐ The Guide

SEARCH

THE ACM DIGITAL LIBRARY

[Feedback](#)

credential index and server and hidden
and sender

Terms used:

[credential index](#) [server](#) [hidden](#) [sender](#)

Found

16 of

248,815

Sort
results
by

relevance

Display
results

expanded form



[Save](#)

[Refine](#)
[these](#)
[results](#)
[to a](#)
[Binder](#)

☐ Open
results
in a new
window

[Advanced](#)

[Search](#)

Try this
search
in [The](#)
[ACM](#)
[Guide](#)

Results 1 - 16 of 16

1 [Delayed password disclosure](#)



Markus Jakobsson, Steven Myers

September 2007 ACM SIGACT News, Volume 38 Issue 3

Publisher: ACM

Full text available: [pdf\(955.13 KB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)


Bibliometrics: Downloads (6 Weeks): 29, Downloads (12 Months): 115, Citation Count: 0

We present a new authentication protocol called Delayed Password Disclosure. Based on the traditional username and password paradigm, the protocol's goal is aimed at reducing the effectiveness of phishing/spoofing attacks that are becoming increasingly ...

Keywords: decisional, doppelganger, oblivious transfer, password authenticated key exchange, phishing, static diffie-hellman, user interfaces

2 Delayed password disclosure

 Markus Jakobsson, Steven Myers
November 2007 DIM '07: Proceedings of the 2007 ACM workshop on Digital identity management
Publisher: ACM

Full text available:  [pdf\(270.28 KB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 128, Citation Count: 0

We present a new authentication protocol called Delayed Password Disclosure. Based on the traditional user name and password paradigm, the protocol's goal is aimed at reducing the effectiveness of phishing/spoofing attacks that are becoming increasingly ...

Keywords: authentication, decisional & static diffie-hellman assumption, oblivious transfer, password authenticated key exchange, phishing, user interfaces

3 Information flow control for standard OS abstractions

 Maxwell Krohn, Alexander Yip, Micah Brodsky, Natan Cliffer, M. Frans Kaashoek, Eddie Kohler, Robert Morris
October 2007 ACM SIGOPS Operating Systems Review, Volume 41 Issue 6
Publisher: ACM

Full text available:  [pdf\(321.86 KB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 31, Downloads (12 Months): 329, Citation Count: 0

Decentralized Information Flow Control (DIFC) is an approach to security that allows application writers to control how data flows between the pieces of an application and the outside world. As applied to privacy, DIFC allows untrusted software to compute ...


Keywords: DIFC, decentralized information flow control, endpoints, reference monitor, system call interposition, web services

4 [Information flow control for standard OS abstractions](#)

 Maxwell Krohn, Alexander Yip, Micah Brodsky, Natan Cliffer, M. Frans Kaashoek, Eddie Kohler, Robert Morris

October 2007 SOSP '07: Proceedings of twenty-first ACM SIGOPS symposium on Operating systems principles

Publisher: ACM

Full text available:  [pdf\(321.86 KB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 31, Downloads (12 Months): 329, Citation Count: 0


Decentralized Information Flow Control (DIFC) is an approach to security that allows application writers to control how data flows between the pieces of an application and the outside world. As applied to privacy, DIFC allows untrusted software to compute ...

Keyw ords: DIFC, decentralized information flow control, endpoints, reference monitor, system call interposition, web services

5 [A secure multicast protocol with copyright protection](#)

 Hao-hua Chu, Lintian Qiao, Klara Nahrstedt, Hua Wang, Ritesh Jain
April 2002 ACM SIGCOMM Computer Communication Review , Volume 32 Issue 2

Publisher: ACM

Full text available:  [pdf\(301.97 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 19, Downloads (12 Months): 138, Citation Count: 2


We present a simple, efficient, and secure multicast protocol with copyright protection in an open and insecure network environment. There is a wide variety of multimedia applications that can benefit from using our secure multicast protocol, e. g., the ...

Keyw ords: copyright protection, key distribution, multicast security, watermark

6 [Role-based access control on the web](#)

 Joon S. Park, Ravi Sandhu, Gail-Joon Ahn
February 2001 ACM Transactions on Information and System Security (TISSEC) , Volume 4 Issue 1

Publisher: ACM

Full text available:  [pdf\(331.03 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#), [review](#)

Bibliometrics: Downloads (6 Weeks): 47, Downloads (12 Months): 408, Citation Count: 23

Current approaches to access control on the Web servers do not scale to enterprise-wide systems because they are mostly based on individual user identities. Hence we were motivated by the need to manage and enforce the strong and efficient RBAC access ...


Keywords: WWW security, cookies, digital certificates, role-based access control

7 Deploying and managing Web services: issues, solutions, and directions

Qi Yu, Xumin Liu, Athman Bouguettaya, Brahim Medjahed

May The VLDB Journal — The International Journal on Very Large Data
2008 Bases, Volume 17 Issue 3

Publisher: Springer-Verlag New York, Inc.

Full text available:  pdf(903.96

KB)

Additional Information: [full citation](#), [abstract](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 61, Downloads (12 Months): 61, Citation Count: 0

Web services are expected to be the key technology in enabling the next installment of the Web in the form of the Service Web. In this paradigm shift, Web services would be treated as first-class ...

Keywords: Interoperability, Service-oriented computing, Web service management system


8 A taxonomy of Data Grids for distributed data sharing, management, and processing



Srikumar Venugopal, Rajkumar Buyya, Kotagiri Ramamohanarao

June ACM Computing Surveys (CSUR), Volume 38 Issue 1
2006

Publisher: ACM

Full text available:  pdf(1.70

MB)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 177, Downloads (12 Months): 1610, Citation Count: 3

Data Grids have been adopted as the next generation platform by many scientific communities that need to share, access, transport, process, and manage large data collections distributed worldwide. They combine high-end computing technologies with high-performance ...

Keywords: Grid computing, data-intensive applications, replica management, virtual organizations

9 [HTTP Cookies: Standards, privacy, and politics](#)



David M. Kristol

November 2001 ACM Transactions on Internet Technology (TOIT), Volume 1 Issue 2

Publisher: ACM

Full text available: [pdf\(390.38 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 60, Downloads (12 Months): 431, Citation Count: 8

How did we get from a world where cookies were something you ate and where "nontechies" were unaware of "Netscape cookies" to a world where cookies are a hot-button privacy issue for many computer users? This article describes how HTTP "cookies" work ...

Keywords: Cookies, HTTP, World Wide Web, privacy, state management

10 [Concealing complex policies with hidden credentials](#)



Robert W. Bradshaw, Jason E. Holt, Kent E. Seamons

October 2004 CCS '04: Proceedings of the 11th ACM conference on Computer and communications security

Publisher: ACM

Full text available: [pdf\(219.13 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 14, Downloads (12 Months): 63, Citation Count: 7

Hidden credentials are useful in protecting sensitive resource requests, resources, policies, and credentials. We propose a significant performance improvement when implementing hidden credentials using Boneh/Franklin Identity Based Encryption. We also ...

Keywords: authentication, credentials, identity based encryption, privacy, secret sharing, trust negotiation

11 [Blind sales in electronic commerce](#)



E. Aïmeur, G. Brassard, F. S. Mani Onana

March 2004 I CEC '04: Proceedings of the 6th international conference on Electronic commerce

Publisher: ACM

Full text available: [pdf\(330.05 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#)

Bibliometrics: Downloads (6 Weeks): 14, Downloads (12 Months): 83, Citation Count: 2

We start with the usual paradigm in electronic commerce: a consumer who wants to buy from a merchant. However, both parties wish to enjoy maximal privacy. In addition to remaining anonymous, the consumer wants to hide her browsing pattern and even the ...


Keywords: CAPTCHA, anonymous surfing, cryptography, customer buying behaviour, electronic commerce, oblivious transfer, private information retrieval

12 Bidirectional mobile code trust management using tamper resistant hardware

John Zachary, Richard Brooks

April Mobile Networks and Applications, Volume 8 Issue 2
2003

Publisher: Kluwer Academic Publishers

Full text available:  [pdf\(152.99 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 4, Downloads (12 Months): 58, Citation Count: 0

Trust management in a networked environment consists of authentication and integrity checking. In a mobile computing environment, both remote hosts and mobile code are suspect. We present a model that addresses trust negotiation between the remote host ...

Keywords: authentication, hash functions, mobile code, tamper resistant hardware, trust management

13 Toward a commodity enterprise middleware



John O'Hara

May 2007 Queue, Volume 5 Issue 4

Publisher: ACM

Full text available:  [pdf\(350.55 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 22, Downloads (12 Months): 299, Citation Count: 0


Can AMQP enable a new era in messaging middleware?

14 [Making p2p accountable without losing privacy](#)

 Mira Belenkiy, Melissa Chase, C. Chris Erway, John Jannotti, Alptekin Küpçü, Anna Lysyanskaya, Eric Rachlin

October 2007 WPES '07: Proceedings of the 2007 ACM workshop on Privacy in electronic society

Publisher: ACM

Full text available:  [pdf\(229.12 KB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 28, Downloads (12 Months): 218, Citation Count: 0

Peer-to-peer systems have been proposed for a wide variety of applications, including file-sharing, web caching, distributed computation, cooperative backup, and onion routing. An important motivation for such systems is self-scaling. That is, increased ...

Keyw ords: anonymity, e-cash, incentives, peer-to-peer, privacy

15 [ID-based encryption for complex hierarchies with applications to forward security and broadcast encryption](#)

 Danfeng Yao, Nelly Fazio, Yevgeniy Dodis, Anna Lysyanskaya
October 2004 CCS '04: Proceedings of the 11th ACM conference on Computer and communications security

Publisher: ACM

Full text available:  [pdf\(220.00 KB\)](#)


Additional Information: [full citation](#), [abstract](#), [references](#), [cited by](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 18, Downloads (12 Months): 106, Citation Count: 2

A forward-secure encryption scheme protects secret keys from exposure by evolving the keys with time. Forward security has several unique requirements in hierarchical identity-based encryption (HIBE) scheme: (1) users join dynamically; (2) encryption ...

Keyw ords: ID-Based encryption, broadcast encryption, forward security

16 [Ordered multisignatures and identity-based sequential aggregate signatures, with applications to secure routing](#)

 Alexandra Boldyreva, Craig Gentry, Adam O'Neill, Dae Hyun Yum
October 2007 CCS '07: Proceedings of the 14th ACM conference on Computer and communications security

Publisher: ACM

Full text available:  [pdf\(342.93 KB\)](#)

Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Bibliometrics: Downloads (6 Weeks): 36, Downloads (12 Months): 218, Citation Count: 0

We construct new multiparty signature schemes that allow multiple signers to sequentially produce a compact, fixed-length signature simultaneously attesting to the message(s) they want to sign. First, we introduce a new primitive that we call *ordered ...*

Results 1 - 16 of 16

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2008 ACM, Inc.

[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)